

Содержание

Detecting DDoS attacks, BotNet activity, and visits to specific resources using triggers in QoE 3

Example: configuring a trigger to detect the source of a Flood-type DDoS attack 3

Example: configuring a trigger to detect the target of a Flood-type DDoS attack 7

BotNet analysis 8

Detecting subscriber visits to competitor resources 9

Detecting DDoS attacks, BotNet activity, and visits to specific resources using triggers in QoE

[Triggers](#) are used to search data in QoE Stor based on specified parameters. When a trigger fires, one of the following actions can occur:

- Notification in GUI
- HTTP action
- Email notification

Required SSG DPI options:

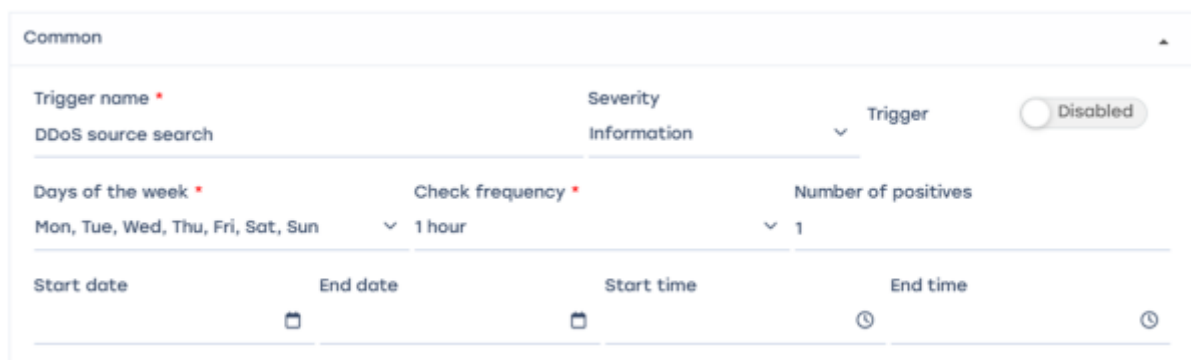
- [Statistics gathering and analysis on protocols and directions](#)
- [Subscriber notifications](#)

Required additional modules:

- [DPIUI2 \(GUI - Graphical User Interface\)](#)
- [Implementation and administration](#)

Example: configuring a trigger to detect the source of a Flood-type DDoS attack

General trigger information



The screenshot shows a configuration window titled 'Common' with a 'Trigger' toggle set to 'Disabled'. The configuration includes the following fields:

Trigger name *		Severity	Trigger
DDoS source search		Information	▼
Days of the week *	Check frequency *	Number of positives	
Mon, Tue, Wed, Thu, Fri, Sat, Sun	1 hour	1	
Start date	End date	Start time	End time

Trigger name: "DDoS source detection", days of the week - all, check frequency - 1 hour, trigger activation frequency - once, start and end times not set.



Every day, the system will perform a check every hour based on the conditions described below.

Queries

Queries						
+						
	Query name	Report		Period from	Period to	
☒ On	A	Maxi		now - 15 minutes	now	

- Add field
- Name: A
- Select table for scanning: Raw full netflow → Tables → Attacks detection → Top hosts IPs → Maxi
- Select period from “now - 15 minutes” to “now”



In this case, the system analyzes traffic for the selected page during the last 15 minutes.

Conditions

Conditions							
+							
	Bind	Query name	Function	Combinator	Serie	Operator	Value
☒ On	AND	A	avg		Session lifetir	<=	20
☒ On	AND	A	avg		Sessions	>=	1500

- Add two "+" fields
- Link - AND
- Function - avg
- Condition 1 - session lifetime <= 20 (ms)
- Condition 2 - number of sessions >= 1500



This means the trigger will fire if sessions with lifetimes ≤ 20 ms AND more than 1500 sessions from the same IP host are detected.

Error handling

No data & error handling	
If no data *	If execution error or timeout *
No data	Keep last state

- “If no errors” — no data
- “If there is an error or timeout” — save last state



In this configuration, no data will be saved if there are no errors, but if errors occur, information about suspicious sessions will be saved as a table.

Actions

E-mail action

Actions

E-mail x

Send to On
your@email.com

Subject
Trigger fired: {trigger.name}

Message  

B I U      Font Size... Font Family... Font Format

Id: {trigger.id}

Trigger: {trigger.name}

Status: {trigger.state}

Severity: {trigger.severity}

Queries:

{trigger.queries}

- Click the "</>" icon to auto-fill the form
- Enter the recipient email address in the “To” field
- When triggered, a notification will be sent to the specified email containing the trigger ID, name, status, and report link (saved state).

Notification

Actions

E-mail x Notification x

Notification title
{trigger.name}

Notification subtitle
{trigger.id}

Notification type
Warning

Message

Id: {trigger.id}
Trigger: {trigger.name}
Status: {trigger.state}
Severity: {trigger.severity}

Queries:
{trigger.queries}

- Click "</>" to auto-fill the form
- Select notification type — "Warning"
- A notification will be created in the SSG system

The report link can be obtained from the notifications menu.

Select the notification Click **Details**

Follow the report link — it will open in a new browser window.

HTTP action

Actions

E-mail x Notification x Http x

Method
POST

Url
https://your_redmine_host/issues.xml?key=your_redmine_api_key

Headers

Name	Value
Content-Type	application/xml

Body

```
<?xml version="1.0"?>
<issue>
  <project_id>1</project_id>
  <subject>Trigger fired: {trigger.name}</subject>
  <priority_id>1</priority_id>
  <description>Id: {trigger.id}\nTrigger: {trigger.name}\nStatus:
{trigger.state}\nSeverity: {trigger.severity}\nQueries:
{trigger.queries}\nReasons for the occurrence of notification:
{trigger.notification.notes}\nLinks to
reports:\n{trigger.report.link}\n\nLinks to
files:\n{trigger.report.csv}\n\n{trigger.report.tsv}\n\n{trigger.report
.xlsx}\n\n{trigger.report.xlsx}</description>
</issue>
```

json Default template
xml Default template

Click "</>" to auto-fill the form, select the method suitable for your ticket system, and enter the URL address.



Keep in mind — values such as session count and packet rate are averaged. Fine-tuning should be performed based on your network specifics.

Example: configuring a trigger to detect the target of a Flood-type DDoS attack

This configuration differs from the previous example in steps 2 and 3 (Queries and Conditions).

Queries

The screenshot shows the 'Queries' configuration section. A dropdown menu is open, showing a search bar and a list of data sources and aggregation methods. The list includes:

- Raw full netflow
- Tables
- Raw log
- Attacks detection
- Top application protocols
- Top application protocols groups
- Top subscribers
- By traffic
- By flow
- By session lifetime
- By subscribers and hosts
- Maxi

The background form shows the following fields:

- Queries:** A table with columns: Query name, Report, Period from, Period to. A row is visible with Query name 'A', Report 'Maxi', Period from 'now - 15 minutes', and Period to 'now'.
- Conditions:** A table with columns: Bind, Operator, Value. Two rows are visible, both with 'AND' in the Bind column, '<=' in the Operator column, and '20' and '1500' in the Value column.
- No data & error handling:** A section with a dropdown menu set to 'No data'.
- Actions:** A section with a dropdown menu set to 'E-mail' and a 'Method' field.

In the report field, select Raw full netflow → Tables → Attacks detection → Top subscribers → Maxi

Conditions

Conditions								
+								
	Bind	Query name	Function	Combinator	Serie	Operator	Value	
☒ On	AND	A	avg		Flow volume t	>=	10000	

Series — “Flow volume to subscribers, Pct/s” >= 10000



Values such as session count and packet rate are averaged. Fine-tuning should be performed based on your network specifics.

BotNet analysis

This configuration differs from the previous example in steps 2 and 3 (Queries and Conditions).

Queries

Queries						
+						
	Query name	Report		Period from	Period to	
☒ On	A	Maxi		now - 15 minutes	now	
☒ On	B	Full raw log		now - 15 minutes	now	

- Select Raw full netflow → Tables → Attacks detection → Top application protocols → Maxi for “A”
- Raw full network → Tables → Raw log → Full raw log for “B”

Conditions

Conditions								
+								
	Bind	Query name	Function	Combinator	Serie	Operator	Value	
☒ On	OR	B	avg		Destination p	=	6667	
☒ On	OR	B	avg		Source port	=	6667	
☒ On	OR	B	avg		Destination p	=	1080	
☒ On	OR	B	avg		Source port	=	1080	
☒ On	AND	A	avg		Flow	>=	2000	

Since BotNet often uses ports 6667 and 1080 — add each destination/source port by selecting query “B” with “OR” condition, and Flow Pcts/s $\geq$ 2000.



In this configuration, the trigger will fire if on any of the ports (6667/1080) the packet rate exceeds 2000 per second.



Values such as session count and packet rate are averaged. Fine-tuning should be performed based on your network specifics.

Detecting subscriber visits to competitor resources

General trigger information

Common			
Trigger name *	Severity	Trigger	
Interest in competitors	Information	▼	☐ Disabled
Days of the week *	Check frequency *	Number of positives	
Mon, Tue, Wed, Thu, Fri, Sat, Sun	▼ 1 hour	▼ 1	
Start date	End date	Start time	End time
			

Trigger name: “Interest in competitors”, days of the week – all, check frequency – 1 hour, trigger activation frequency – once, start and end times not set.



Every day, the system will perform a check every hour based on the conditions described below.

Queries

Queries						
+						
	Query name	Report		Period from	Period to	
☒ On	A	Raw clickstream	▼	now - 1 hour	now	🗑
☒ On	B	Maxi	▼	now - 1 hour	now	🗑

- Add “+” field
- Name A — select table: Raw clickstream → Tables → Raw clickstream
- Name B — select table: Raw full netflow → Tables → Attacks detection → Top hosts IPs → Maxi
- Select period from “now - 1 hour” to “now”
- This setup analyzes traffic hourly based on the selected tables.

Conditions

Conditions								
+								
	Bind	Query name	Function	Combinator	Serie	Operator	Value	
☒ On	OR	A	avg		Host	=	*megafon.ru	🗑
☒ On	AND	B	avg		Flow volume f	>=	800	🗑
☒ On	OR	A	avg		Host	=	*mts.ru	🗑

- Add 3 “+” fields
- First field — select table “A”; Link - “OR”; Function - “avg”; Series Host = *megafon.ru (or your competitor)
- Second field — select table “B”; Link - “AND”; Function - “avg”; Series Flow volume from subscriber, Pct/s >= 800



The trigger will fire if at least 800 packets (indicating a meaningful visit) from a subscriber to a competitor’s website are detected.

Error handling

No data & error handling	
If no data *	If execution error or timeout *
No data	Keep last state

- “If no errors” — no data
- “If there is an error or timeout” — save last state



In this configuration, no data will be saved if there are no errors, but if errors occur, information about suspicious sessions will be saved as a table.

Actions

E-mail action

Actions

E-mail

Send to

your@email.com

Subject

Trigger fired: {trigger.name}

Message

Id: {trigger.id}

Trigger: {trigger.name}

Status: {trigger.state}

Severity: {trigger.severity}

Queries:

{trigger.queries}

- Click to auto-fill the form
- Enter recipient email address in “To” field



When triggered, an email containing notification details — ID, trigger name, status, and report link (saved state) — will be sent to the specified address.

Notification

Actions

E-mail x Notification x

Notification title
{trigger.name}

Notification subtitle
{trigger.id}

Notification type
Warning

Message

Id: {trigger.id}
Trigger: {trigger.name}
Status: {trigger.state}
Severity: {trigger.severity}

Queries:
{trigger.queries}

- Click "</>" to auto-fill the form
- Select notification type — "Warning"
- A notification will be created in the SSG system

The report link can be obtained from the notifications menu.

Select the notification Click **Details**

Follow the report link — it will open in a new browser window.

HTTP action

Actions

E-mail x Notification x Http x

Method
POST

Url
https://your_redmine_host/issues.xml?key=your_redmine_api_key

Headers

Body

Content-Type
application/xml

json Default template
xml Default template

```
<?xml version="1.0"?>
<issue>
  <project_id>1</project_id>
  <subject>Trigger fired: {trigger.name}</subject>
  <priority_id>1</priority_id>
  <description>Id: {trigger.id}\nTrigger: {trigger.name}\nStatus:
{trigger.state}\nSeverity: {trigger.severity}\nQueries:
{trigger.queries}\nReasons for the occurrence of notification:
{trigger.notification.notes}\nLinks to
reports:\n{trigger.report.link}\n\nLinks to
files:\n{trigger.report.csv}\n\n{trigger.report.tsv}\n\n{trigger.report
.xlsx}\n\n{trigger.report.xlsx}</description>
</issue>
```

- Click "</>" to auto-fill the form
- Select the method suitable for your ticket system and enter the URL address



Keep in mind — values such as session count and packet rate are averaged. Fine-tuning should be performed based on your network specifics.